10019968-2

Reference 1

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-244478

(43)Date of publication of application : 08.09.2000

(51)Int.Cl.	H04L 9/08 G09C 1/00 H04L 9/32

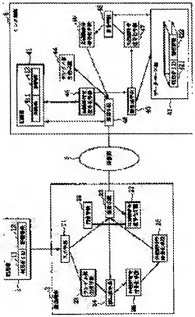
(21)Application number :	11-044279	(71)Applicant :	NIPPON TELEGR & TELEPH CORP <NTT>
(22)Date of filing :	23.02.1999	(72)Inventor :	SHIMAMURA YUICHI AOKI TAKAHIRO

(54) METHOD FOR USER AUTHENTICATION/KEY SHARING

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a user authentication/key sharing method by which user authentication and key sharing can be conducted through a communication network where interception and pretence may be in existence without the need for provision of a privately shared key and a private key encrypted by a public key to users and communication terminals or for installation of an authentication station.

SOLUTION: A communication terminal 2 uses a public key 411 adopting a public key encryption received from a center device 4 to encrypt a user ID, transmits the encrypted ID to the center device 4, the center device 4 retrieves private information (password or the like) on the basis of the encrypted user ID, generates a key adopting a common key encryption between the communication terminal 2 and the center device 4 on the basis of private information 12 entered to the communication terminal 2 by a user, or private information 422 retrieved by the center device 4, a random value generated by the communication terminal 2 and a random value generated by the center device 4, encrypts the user ID and the private information by using the shared key, the communication terminal 2 transmits the result to the center device 4, where combination between the user ID and the private information is collated for authentication.


4
41
411
412
42
421
422
43
44
45
46
47
48
49
5
1
11
12
2
21
22
23
24
25
26
27
28